

The Whitehead group of (almost) extra-special p -groups with p odd

Serge Bouc¹ and Nadia Romero²

Abstract: Let p be an odd prime number. We describe the Whitehead group of all extra-special and almost extra-special p -groups. For this we compute, for any finite p -group P , the subgroup $Cl_1(\mathbb{Z}P)$ of $SK_1(\mathbb{Z}P)$, in terms of a genetic basis of P . We also introduce a deflation map $Cl_1(\mathbb{Z}P) \rightarrow Cl_1(\mathbb{Z}(P/N))$, for a normal subgroup N of P , and show that it is always surjective. Along the way, we give a new proof of the result describing the structure of $SK_1(\mathbb{Z}P)$, when P is an elementary abelian p -group.

Keywords: Whitehead group, almost extra-special p -groups, genetic basis.

MSC2010: 19B28, 20C05, 20D15.

Introduction

Whitehead groups were introduced by J.H.C. Whitehead in [19], as an algebraic continuation of his work on combinatorial homotopy. The computation of the Whitehead group $Wh(G)$ of a finite group G is in general very hard, and a compendium on the subject is the book by Bob Oliver ([13]) of 1988. Since then, it seems that not much progress has been made on this subject (see however [12], [11], [18], [17]).

Let p be an odd prime number. In this paper, we describe the Whitehead group of all extra-special and almost extra-special p -groups. The main reason for focusing on these p -groups is that, apart from elementary abelian p -groups, they are exactly the finite p -groups all proper factor groups of which are elementary abelian (see e.g. Lemma 3.1 of [8]). In particular these groups appear naturally in various areas as first crucial step in inductive procedures (see [8], [7], or the proof of Serre's Theorem in Section 4.7 of [3] for examples).

One of the main tools in our method is Theorem 9.5 of [13], which gives a first description, for a finite p -group P , of the subgroup $Cl_1(\mathbb{Z}P)$, an essential part of the torsion of $Wh(P)$. In addition to this, we make use of *biset functor* techniques, in two

¹CNRS-LAMFA, UPJV, Amiens, France

²DEMAT, UGTO, Guanajuato, Mexico - Partially supported by SEP-PRODEP, project PTC-486

different ways: first we use *genetic bases* of finite p -groups. They allow for an explicit combinatorial description of the rational irreducible representations of P . This yields a description of $Cl_1(\mathbb{Z}P)$, in terms of a genetic basis of P . Next we show that for any normal subgroup N of P , there is a *deflation operation* $\text{Def}_{P/N}^P : Cl_1(\mathbb{Z}P) \rightarrow Cl_1(\mathbb{Z}(P/N))$. Even if there seems to be no inflation operation in the other direction, which would provide a section of this map, we show that $\text{Def}_{P/N}^P$ is always surjective.

In the case of an extra-special or almost extra-special p -group P , the group $Cl_1(\mathbb{Z}P)$ is equal to the torsion part $SK_1(\mathbb{Z}P)$ of $Wh(P)$, so the computation of the Whitehead group of P comes down to the knowledge of $Cl_1(\mathbb{Z}(P/\Phi(P)))$, where $\Phi(P)$ is the Frattini subgroup of P , and a detailed analysis of what happens with the unique faithful rational irreducible representation of P . It should be noted that our methods not only give the algebraic structure of the Whitehead group, but allow also for the determination of explicit generators of its torsion subgroup.

The paper is organized as follows: Section 1 is a review of definitions and basic results on Whitehead groups, genetic bases of p -groups, extra-special and almost extra-special p -groups. In particular, the subgroups $Cl_1(\mathbb{Z}G)$ and $SK_1(\mathbb{Z}G)$ of the Whitehead group $Wh(G)$ of a group G are introduced. In Section 2, we give a procedure (Theorem 2.4) to compute $Cl_1(\mathbb{Z}P)$ for a finite p -group P (with p odd) in terms of a genetic basis of P . This procedure may be of independent interest, in particular from an algorithmic point of view. Finally, in Section 3, we begin by giving a new proof of the structure of $Wh(P)$ for an elementary abelian p -group P , for p odd, and then we come to our main theorems (Theorem 3.17 and Theorem 3.20), which give the structure of $Wh(P)$, when P is an extra-special or almost extra-special p -group, for p odd.

1. Preliminaries

Let G be a group. We will write $Z(G)$ for the center of G and G' for its commutator subgroup. The Frattini subgroup of G is denoted by $\Phi(G)$. If H is a subgroup of G , the normalizer of H in G will be denoted by $N_G(H)$, and its centralizer by $C_G(H)$. If $H = \langle h \rangle$ for an element $h \in G$, we may also write $C_G(H) = C_G(h)$.

1.1. About the Whitehead group.

Let R be an associative ring with unit. The infinite general linear group of R , denoted by $GL(R)$, is defined as the direct limit of the inclusions $GL_n(R) \rightarrow GL_{n+1}(R)$ as the upper left block matrix. If, for each $n > 0$, we denote by $E_n(R)$ the subgroup of

$GL_n(R)$ generated by all elementary $n \times n$ -matrices – i.e. all those which are the identity except for one non-zero off-diagonal entry – and we take the direct limit as before for the groups $E_n(R)$, we obtain a subgroup of $GL(R)$, denoted by $E(R)$. Whitehead's Lemma states that $E(R)$ is equal to the derived subgroup of $GL(R)$. The group $K_1(R)$ is defined as the abelianization of $GL(R)$, which is then equal to $GL(R)/E(R)$.

If G is a group and we take R as the group ring $\mathbb{Z}G$, then elements of the form $\pm g$ for $g \in G$ can be regarded as invertible 1×1 -matrices over $\mathbb{Z}G$ and hence they represent elements in $K_1(\mathbb{Z}G)$. Let H be the subgroup of $K_1(\mathbb{Z}G)$ generated by classes of elements of the form $\pm g$ with $g \in G$. The *Whitehead group* of G is defined as $Wh(G) = K_1(\mathbb{Z}G)/H$.

If G is finite, the groups $K_1(\mathbb{Z}G)$ and $Wh(G)$ are finitely generated abelian groups.

For the rest of this section, G denotes a finite group.

1.2. Definition. *Let D be an integral domain and K be its field of fractions, then $SK_1(DG)$ denotes the kernel of the morphism*

$$K_1(DG) \rightarrow K_1(KG).$$

By Theorem 7.4 in [13], $SK_1(\mathbb{Z}G)$ is isomorphic to the torsion subgroup of $Wh(G)$. Hence, $Wh(G)$ is completely determined by $SK_1(\mathbb{Z}G)$ and the rank of its free part (i.e. its *free rank*). According to Theorem 2.6 in [13], this free rank is equal to $r - q$, where r is the number of non-isomorphic irreducible \mathbb{R} -representations of G and q is the number of non-isomorphic irreducible \mathbb{Q} -representations of G .

1.3. Definition. *Consider the ring of p -adic integers $\hat{\mathbb{Z}}_p$. The group $Cl_1(\mathbb{Z}G)$ is defined as the kernel of the localization morphism*

$$l : SK_1(\mathbb{Z}G) \rightarrow \bigoplus_p SK_1(\hat{\mathbb{Z}}_p G).$$

By Theorem 3.9 in [13], $SK_1(\hat{\mathbb{Z}}_p G)$ is trivial whenever p does not divide $|G|$, and l is onto. In particular, $SK_1(\mathbb{Z}G)$ sits in an extension

$$0 \longrightarrow Cl_1(\mathbb{Z}G) \longrightarrow SK_1(\mathbb{Z}G) \longrightarrow \bigoplus_p SK_1(\hat{\mathbb{Z}}_p G) \longrightarrow 0.$$

This extension is used by Oliver in [13] to describe $SK_1(\mathbb{Z}G)$ in many cases. The important feature of the examples treated in this paper is that they all satisfy that $\bigoplus_p SK_1(\hat{\mathbb{Z}}_p G)$ is trivial, and so describing $SK_1(\mathbb{Z}G)$ amounts to describing $Cl_1(\mathbb{Z}G)$.

1.4. About genetic bases.

A finite p -group Q is called a *Roquette p -group* if it has normal p -rank 1, i.e. if all its abelian normal subgroups are cyclic. The Roquette p -groups (see [15] or Theorem 4.10 of [10] for details) of order p^n are the cyclic groups C_{p^n} , if p is odd, and the cyclic groups C_{2^n} , the generalized quaternion groups Q_{2^n} , for $n \geq 3$, the dihedral groups D_{2^n} , for $n \geq 4$, and the semidihedral groups SD_{2^n} , for $n \geq 4$, if $p = 2$. A Roquette p -group Q admits a unique rational irreducible representation Φ_Q (see e.g. Proposition 9.3.5 in [5]).

1.5. Definition. *Let P be a finite p -group. A subgroup S of P is called genetic if the section $S \trianglelefteq N_P(S) \leq P$ satisfies*

1. *The group $N_P(S)/S$ is a Roquette group.*
2. *Let $\Phi = \Phi_{N_P(S)/S}$ be the only faithful irreducible \mathbb{Q} -representation of $N_P(S)/S$ and $V = \text{Ind}_{N_P(S)}^P \text{Inf}_{N_P(S)/S}^{N_P(S)} \Phi$, then the functor $\text{Ind}_{N_P(S)}^P \text{Inf}_{N_P(S)/S}^{N_P(S)}$ induces an isomorphism of \mathbb{Q} -algebras*

$$\text{End}_{\mathbb{Q}P} V \cong \text{End}_{\mathbb{Q}(N_P(S)/S)} \Phi.$$

Note that the right-hand side algebra is actually a skew field by Schur's lemma. So $\text{End}_{\mathbb{Q}P} V$ is also a skew field, hence V is an indecomposable – that is, irreducible – $\mathbb{Q}P$ -module.

1.6. Notation. *Let P be a finite p -group and S be a genetic subgroup of P . We write*

$$V(S) = \text{Ind}_{N_P(S)}^P \text{Inf}_{N_P(S)/S}^{N_P(S)} \Phi_{N_P(S)/S}.$$

Then $V(S)$ is an irreducible \mathbb{Q} -representation of P . Conversely, by Roquette's Theorem (Theorem 9.4.1 in [5]), for each irreducible \mathbb{Q} -representation V of P , there exists a genetic subgroup S of P such that $V \cong V(S)$.

The following theorem characterizes the genetic subgroups of a p -group. First some notation: for a subgroup S of a finite p -group P , let $Z_P(S) \geq S$ be the subgroup of $N_P(S)$ defined by $Z_P(S)/S = Z(N_P(S)/S)$. In particular $Z_P(S) = N_P(S)$ if $N_P(S)/S$ is abelian, e.g. if $N_P(S)/S$ is a Roquette p -group for p odd.

1.7. Theorem. *[Theorem 9.5.6 in [5]] Let P be a finite p -group and S be a subgroup of P such that $N_P(S)/S$ is a Roquette group. Then the following conditions are equivalent:*

1. *The subgroup S is a genetic subgroup of P .*
2. *If $x \in P$ is such that ${}^x S \cap Z_P(S) \leq S$, then ${}^x S = S$.*
3. *If $x \in P$ is such that ${}^x S \cap Z_P(S) \leq S$ and $S^x \cap Z_P(S) \leq S$, then ${}^x S = S$.*

The next result is part of Theorem 9.6.1 in [5].

1.8. Theorem. *Let P be a finite p -group and S and T be genetic subgroups of P . The following conditions are equivalent:*

1. *The $\mathbb{Q}P$ -modules $V(S)$ and $V(T)$ are isomorphic.*
2. *There exist $x, y \in P$ such that ${}^xT \cap Z_P(S) \leq S$ and ${}^yS \cap Z_P(T) \leq T$.*
3. *There exists $x \in P$ such that ${}^xT \cap Z_P(S) \leq S$ and $S^x \cap Z_P(T) \leq T$.*

If these conditions hold, then in particular the groups $N_P(S)/S$ and $N_P(T)/T$ are isomorphic.

The relation between groups appearing in point 2 is denoted by $S \trianglelefteq_P T$. The theorem shows that this relation is an equivalence relation on the set of genetic subgroups of P , and we have the following definition.

1.9. Definition. *[Definition 9.6.11 in [5]] Let P be a finite p -group. A genetic basis of P is a set of representatives of the equivalence classes of \trianglelefteq_P in the set of genetic subgroups of P .*

1.10. Lemma. *Let P be a finite p -group and S be a genetic subgroup of P .*

1. *The kernel of $V(S)$ is equal to the intersection of the conjugates of S in P .*
2. *In particular $V(S)$ is faithful if and only if S intersects $Z(P)$ trivially.*

Proof. Denote by Φ the unique rational irreducible representation of the Roquette group $N_P(S)/S$. Then

$$V(S) = \text{Ind}_{N_P(S)}^P \text{Inf}_{N_P(S)/S}^{N_P(S)} \Phi \cong \bigoplus_{x \in [P/N_P(S)]} x \otimes \Phi,$$

where $[P/N_P(S)]$ is a chosen set of representatives of $N_P(S)$ -cosets in P . An element $g \in P$ acts trivially on $V(S)$ if and only if it permutes trivially the summands of this decomposition, that is if $g^x \in N_G(S)$ for any $x \in G$, and if moreover g^x acts trivially on Φ , which means that $g^x \in S$, since Φ is faithful. This proves Assertion 1.

Assertion 2 follows, since

$$\left(\bigcap_{x \in P} {}^xS \right) \cap Z(P) = \bigcap_{x \in P} ({}^xS \cap Z(P)) = \bigcap_{x \in P} {}^x(S \cap Z(P)) = S \cap Z(P),$$

and since the normal subgroup $\bigcap_{x \in P} {}^xS$ of P is trivial if and only if it intersects $Z(P)$ trivially. □

1.11. Remark. If P is abelian, then a subgroup S of P is genetic if and only if P/S is cyclic. Moreover the relation \trianglelefteq_P is the equality relation in this case, so there is a unique genetic basis of P , consisting of all the subgroups S of P such that P/S is cyclic.

1.12. Remark. Let P be a finite p -group, and S be a subgroup of P such that $N_P(S)$ is normal in P . If $N_P(S)/S$ is a Roquette group, then S is a genetic subgroup of P . Indeed if $N_P(S)$ is normal in P , then $N_P(S) = N_P({}^xS)$ for any $x \in P$. Hence ${}^xS \trianglelefteq N_P(S)$, and the group ${}^xS \cdot S/S$ is a normal subgroup of $N_P(S)/S$. It is trivial if and only if it intersects trivially the center $Z_P(S)/S$ of $N_P(S)/S$. Then

$$\begin{aligned} {}^xS = S &\iff {}^xS \cdot S/S = \mathbf{1} &\iff {}^xS \cdot S \cap Z_P(S) = ({}^xS \cap Z_P(S))S = S \\ &&\iff {}^xS \cap Z_P(S) \leq S. \end{aligned}$$

1.13. About extra-special and almost extra-special p -groups.

1.14. Definition. Let p be a prime and P be a finite p -group.

1. The group P is called *extra-special* if $Z(P) = P' = \Phi(P)$ has order p .
2. The group P is called *almost extra-special* if $P' = \Phi(P)$ has order p and $Z(P)$ is cyclic of order p^2 .

Extra-special and almost extra-special p -groups can be classified in the following way.

1.15. Notation. Let H , K and M be groups such that $M \leq Z(H)$ and such that there exists an injective map $\theta : M \rightarrow Z(K)$. The central product of H and K with respect to θ will be denoted by $H *_\theta K$, and simply by $H * K$ if θ is clear from the context.

For any integer $r \geq 1$, we will write H^{*r} for the central product of r copies of the group H , where $M = Z(H)$, with the convention $H^{*1} = H$.

For $p \neq 2$, set

$$M(p) = \langle x, y \mid x^p = y^p = 1, [x^{-1}, y] = [y, x] = {}^y[y, x] \rangle$$

and

$$N(p) = \langle x, y \mid x^{p^2} = y^p = 1, {}^yx = x^{1+p} \rangle.$$

1.16. Theorem. *Let p be a prime and P be a finite p -group.*

1. *If P is extra-special, then there exists an integer $r \geq 1$ such that P has order p^{2r+1} and P is isomorphic to only one of the following groups: D_8^{*r} or $Q_8 * D_8^{*(r-1)}$ if $p = 2$, and $M(p)^{*r}$ or $N(p) * M(p)^{*(r-1)}$ if $p \neq 2$.*
2. *If P is almost extra-special, then there exists an integer $r \geq 1$ such that P has order p^{2r+2} and P is isomorphic to only one of the following groups: $D_8^{*r} * C_4$ if $p = 2$, and $M(p)^{*r} * C_{p^2}$ if $p \neq 2$.*

Proof. The proof of 1 can be found in Section 5.5 of [10]. As for point 2, one can refer to Sections 2 and 4 of [8]. \square

Observe that if p is odd, the exponent of the group characterizes the isomorphism type of extra-special p -groups, one of them has exponent p and the other one has exponent p^2 .

If P is an (almost) extra-special group, the quotient P/P' is elementary abelian, so it can be regarded as a (finite-dimensional) vector space E over the finite field \mathbb{F}_p . Moreover, if we take z a generator of P' , then E is endowed with a bilinear form

$$b : E \times E \rightarrow \mathbb{F}_p,$$

that sends an element (u, v) to $b(u, v)$, the element of \mathbb{F}_p satisfying $[\tilde{u}, \tilde{v}] = z^{b(u, v)}$ for all $\tilde{u} \in u, \tilde{v} \in v$ and $u, v \in E$. This bilinear form is alternating, i.e. $b(v, v) = 0$ for all $v \in E$, hence it is antisymmetric, i.e. $b(u, v) = -b(v, u)$ for all $u, v \in E$. Section 20 in [9] is concerned with this bilinear form for extra-special groups, but the property of being alternating is called *symplectic*.

Recall that if $f : V \times V \rightarrow K$ is a bilinear form on a finite dimensional vector space V over a field K , its *left radical* V^\perp is defined by $V^\perp = \{v \in V \mid f(v, w) = 0 \forall w \in V\}$, and its *right radical* by ${}^\perp V = \{v \in V \mid f(w, v) = 0 \forall w \in V\}$. Clearly $V^\perp = {}^\perp V$ when f is antisymmetric. The *rank* of f is the codimension of V^\perp . The form f is called *non-degenerate* if $V^\perp = \{0\}$.

With the help of Lemma 20.4 in [9], we have the following observation.

1.17. Observation. *The bilinear form b is non-degenerate if and only if P is extra-special. If P is almost extra-special, then $E^\perp = \pi(Z(P))$ is a line in E , where $\pi : P \rightarrow P/P'$ is the projection morphism.*

In section 3.2 we will use the following result, which is part of Lemma 2.6 in [7]. For the proof we refer the reader to this reference.

1.18. Lemma. *Let P be an (almost) extra-special p -group, and let Q be a non-trivial subgroup of P . Then*

1. $Q \trianglelefteq P \Leftrightarrow P' \leq Q$.
2. *If Q is not normal in P , then $N_P(Q) = C_P(Q)$. In particular, it follows that in this case Q is elementary abelian of rank at most r , for the integer r defined as in Theorem 1.16, and we have $|Q||C_P(Q)| = |P|$. Moreover, $C_P(Q) = Q \times U$, where U is (almost) extra-special of order $|P|/|Q|^2$ or $U = Z(P)$.*

2. Cl_1 of finite p -group algebras for odd p

The goal of this section is to re-write Theorem 9.5 in [13] in terms of genetic bases, in the most possible succinct way. We take the statement of this theorem appearing in Section 1 of [14], which says the following: let p be an odd prime, let P be a finite p -group, and write $\mathbb{Q}P \cong \prod_{i=1}^k A_i$, where A_i is simple with irreducible module V_i and center $K_i = \text{End}_{\mathbb{Q}P} V_i$. By Roquette's Theorem, for each $1 \leq i \leq k$, the field K_i is isomorphic to $\mathbb{Q}(\zeta_{r_i})$, where ζ_{r_i} is a primitive p^{r_i} -th root of unity for some non-negative r_i , and A_i is isomorphic to a matrix algebra over $\mathbb{Q}(\zeta_{r_i})$.

Consider the abelian group $T = \prod_{i=1}^k \langle \zeta_{r_i} \rangle$. For each $h \in P$, define

$$\psi_h : C_P(h) \rightarrow T, \quad \psi_h(g) = (\det_{K_i}(g, V_i^h))_i$$

where $V_i^h = \{x \in V_i \mid hx = x\}$. Here V_i^h is viewed as a $K_i C_P(h)$ -module, so $\det_{K_i}(g, V_i^h)$ is the determinant (in K_i) of the action of g in V_i^h . Since P is a p -group, this determinant is in $\langle \zeta_{r_i} \rangle$. Then Theorem 9.5 in [13] can be written in the following way.

2.1. Theorem. *Let p be an odd prime and consider T and $\psi_h : C_P(h) \rightarrow T$, for each $h \in P$, as before. Then*

$$Cl_1(\mathbb{Z}P) \cong T / \langle \text{Im} \psi_h \mid h \in P \rangle.$$

Now, since p is odd, if we let $\mathcal{S} = \{S_1, \dots, S_k\}$ be a genetic basis of P , then $N_P(S_i)/S_i$ is cyclic for every $1 \leq i \leq k$ and each simple $\mathbb{Q}P$ -module V_i is isomorphic to $V(S_i) = \text{Indinf}_{N_P(S_i)/S_i}^P \Phi_{N_P(S_i)/S_i}$. Then the abelian group T defined before is isomorphic to $\Gamma(P) = \prod_{i=1}^k (N_P(S_i)/S_i)$. This is because we can see the module $\Phi_{N_P(S_i)/S_i} \cong \mathbb{Q}(\zeta_{r_i})$, where $p^{r_i} = |N_P(S_i)/S_i|$ as actually being generated by a generator of $N_P(S_i)/S_i$ and thus the action of $N_P(S_i)/S_i$ on it can be seen as multiplication

on the group. In particular, $\det_{K_i}(g, V_i^h)$, which is an element of the field K_i , can be regarded as an element in $N_P(S_i)/S_i$. The first step in re-writing Theorem 2.1 is to find this element, for every S_i , every element $h \in P$ and every $g \in C_P(h)$.

2.2. Notation. Let p be an odd prime. If V is a simple $\mathbb{Q}P$ -module and S is a genetic subgroup of P corresponding to V , we will write $\det_{N_P(S)/S}(g, V^h)$ for the element in $N_P(S)/S$ corresponding to $\det_K(g, V^h)$, where $K = \text{End}_{\mathbb{Q}P}(V)$.

2.3. Lemma. Suppose p is an odd prime. Let V be a simple $\mathbb{Q}P$ -module and S be a genetic subgroup of P corresponding to V . Take an element h in P . Let $H = \langle h \rangle$ and $[H \backslash P / N_P(S)]$ be a set of representatives of the double cosets of P on H and $N_P(S)$. Then, for $g \in C_P(H)$, we have

$$\det_{N_P(S)/S}(g, V^h) = \prod_{\substack{x \in [H \backslash P / N_P(S)] \\ \text{s.t. } H^x \cap N_P(S) \leq S}} \overline{n_{g,x}},$$

where $n_{g,x}$ is an element in $N_P(S)$ given by the action σ_g of g in $[H \backslash P / N_P(S)]$, that is $gx = h_{g,x}\sigma_g(x)n_{g,x}$, with $h_{g,x} \in H$ and $\sigma_g(x) \in [H \backslash P / N_P(S)]$ (even though the element $n_{g,x}$ may not be unique, its class in $N_P(S)/S$ is, thanks to the conditions on x).

Proof. Set Φ for $\Phi_{N_P(S)/S}$. Let $[P/N_P(S)]$ be a set of representatives of the cosets of P in $N_P(S)$. Since $V \cong \text{Indinf}_{N_P(S)/S}^P \Phi$, we can write it as $\bigoplus_{a \in [P/N_P(S)]} a \otimes \Phi$. The action of

$y \in P$ is given by $y(a \otimes \omega) = ya \otimes \omega$, which is equal to $\tau_y(a) \otimes \overline{n_{y,a}}\omega$, if $ya = \tau_y(a)n_{y,a}$ for a corresponding $n_{y,a}$ in $N_P(S)$, with $\overline{n_{y,a}}$ being its class in $N_P(S)/S$.

If $y \in H$ fixes an element $u = \sum_{a \in [P/N_P(S)]} a \otimes \omega_a$ of V , we have

$$\sum_{a \in [P/N_P(S)]} \tau_y(a) \otimes \overline{n_{y,a}}\omega_a = \sum_{a \in [P/N_P(S)]} a \otimes \omega_a = \sum_{a \in [P/N_P(S)]} \tau_y(a) \otimes \omega_{\tau_y(a)}.$$

That is, for every $a \in [P/N_P(S)]$ we should have $\overline{n_{y,a}}\omega_a = \omega_{\tau_y(a)}$. If $\tau_y(a) = a$, then we should have that y is in $H \cap {}^a N_P(S)$ and that $H^a \cap N_P(S) \leq S$, if ω_a is different from zero. We consider then the set $[H \backslash P / N_P(S)]$ and we have that

$$u = \sum_{\substack{x \in [H \backslash P / N_P(S)] \\ \text{s.t. } H^x \cap N_P(S) \leq S}} \sum_{z \in [H / H \cap {}^x N_P(S)]} zx \otimes \omega_x.$$

This means that a \mathbb{Q} -basis for V^h is given by $\mu_{x,\omega} = \sum_{z \in [H / H \cap {}^x N_P(S)]} zx \otimes \omega$ with x running over $F = \{x \in [H \backslash P / N_P(S)] \mid H^x \cap N_P(S) \leq S\}$ and ω running over a \mathbb{Q} -basis of Φ . Since $\Phi \cong \mathbb{Q}(\zeta_r) \cong \text{End}_{\mathbb{Q}P}(V)$, where ζ_r is a primitive p^r -th root of unity,

if the order of $N_P(S)/S$ is p^r , then a $\mathbb{Q}(\zeta_r)$ -basis of V^h is the set of $\mu_x = \mu_{x,1}$ with x running over F .

Now, for μ_x we have that $g\mu_x$ is equal to

$$\sum_{z \in [H/H \cap^x N_P(S)]} zh_{g,x}\sigma_g(x) \otimes \overline{n_{g,x}} 1$$

if $gx = h_{g,x}\sigma_g(x)n_{g,x}$. That is

$$g\mu_{x,1} = h_{g,x}\mu_{\sigma_g(x),\overline{n_{g,x}}} = \mu_{\sigma_g(x),\overline{n_{g,x}}},$$

since $\mu_{\sigma_g(x),\overline{n_{g,x}}}$ is in V^h . So we can write $g\mu_x = \overline{n_{g,x}}\mu_{\sigma_g(x)}$, with $\overline{n_{g,x}}$ seen as an element in the field $\mathbb{Q}(\zeta_r)$. This implies that the action of g in V^h is given by a monomial matrix A , the coefficient in the non-zero entry of a row being $\overline{n_{g,x}}$. Then, the determinant of A is the product of the signature of the permutation σ_g by the product of the coefficients $\overline{n_{g,x}}$. Since p is odd, the signature is $+1$, and

$$\det(A) = \prod_{\substack{x \in [H \setminus P/N_P(S)] \\ \text{s.t. } H^x \cap N_P(S) \leq S}} \overline{n_{g,x}}.$$

□

Our final version of Theorem 2.1 is the following.

2.4. Theorem. *Let p be an odd prime and P be a finite p -group. Take a set \mathcal{C} of representatives of conjugacy classes of cyclic subgroups of P . For each $H \in \mathcal{C}$, let \overline{E}_H be a generating set of the factor group $C_P(H)/H$ and $E_H \subseteq C_P(H)$ be a set of representatives of the classes $gH \in \overline{E}_H$. Let also \mathcal{S} be a genetic basis of P and for each $S \in \mathcal{S}$, let $[H \setminus P/N_P(S)]$ be a set of representatives of the double cosets of P on H and $N_P(S)$. Then*

$$Cl_1(\mathbb{Z}P) \cong \left(\prod_{S \in \mathcal{S}} (N_P(S)/S) \right) / \mathcal{R},$$

where \mathcal{R} is the subgroup generated by the elements $u_{H,g} = (u_{H,g,S})_{S \in \mathcal{S}}$, for $H \in \mathcal{C}$ and $g \in E_H$, with

$$u_{H,g,S} = \prod_{\substack{x \in [H \setminus P/N_P(S)] \\ \text{s.t. } H^x \cap N_P(S) \leq S}} \overline{n_{g,x}}$$

where $n_{g,x}$ is an element in $N_P(S)$ given by the action σ_g of g on $[H \setminus P/N_P(S)]$, that is $gx = h_{g,x}\sigma_g(x)n_{g,x}$, for $h_{g,x} \in H$ and $\sigma_g(x) \in [H \setminus P/N_P(S)]$.

Proof. As we said at the beginning of the section, since p is odd, we have $Cl_1(\mathbb{Z}P) \cong \Gamma(P)/\mathcal{R}$, where

$$\Gamma(P) = \prod_{S \in \mathcal{S}} (N_P(S)/S)$$

and \mathcal{R} is the subgroup generated by all the elements $u_{h,g} = (u_{h,g,S})_{S \in \mathcal{S}}$, with $g \in C_P(h)$ and $u_{h,g,S} = \det_{N_P(S)/S}(g, V(S)^h)$, where $V(S) = \text{Indinf}_{N_P(S)/S}^P \Phi_{N_P(S)/S}$.

We first observe that $u_{h,g} = u_{yhy^{-1}, ygy^{-1}}$, for any $y \in G$. Indeed, setting $V = V(S)$, we have a commutative diagram

$$\begin{array}{ccc} V^h & \xrightarrow{g} & V^h \\ y \downarrow & & \downarrow y \\ V^{yh} & \xrightarrow{ygy^{-1}} & V^{yh} \end{array}$$

where the arrows are given by the actions of the labelling elements. It follows that the determinant of ygy^{-1} acting on V^{yh} is equal to the determinant of g acting on V^h . Hence to generate the subgroup \mathcal{R} of $\Gamma(P)$, it suffices to take the elements $u_{h,g}$, where (h, g) runs through a set of representatives of conjugacy classes of pairs of commuting elements in P .

Now clearly for each $h \in H$, the map $g \mapsto u_{h,g}$ is a group homomorphism from $C_P(h)$ to $\Gamma(P)$, hence \mathcal{R} is generated by the elements $u_{h,g}$, where $h \in P$ and g runs through a set of generators of $C_P(h)$. Moreover, as h acts as the identity on V^h , the group generated by h is contained in the kernel of this morphism.

Finally, by Lemma 2.3, setting $H = \langle h \rangle$, we have

$$u_{h,g,S} = \prod_{\substack{x \in [H \backslash P / N_P(S)] \\ \text{s.t. } H^x \cap N_P(S) \leq S}} \overline{n_{g,x}}$$

and this depends only on H , so we may denote it by $u_{H,g,S}$, and by $u_{H,g}$ the corresponding element of $\Gamma(P)$.

It follows that \mathcal{R} is generated by the elements $u_{H,g}$, where H is a cyclic subgroup of P up to conjugation, and for a given H , the element g runs through a subset of $C_P(H)$ which, together with H , generates $C_P(H)$. This completes the proof. \square

To finish the section, we prove that if N is a normal subgroup of a finite p -group P with p odd, then there is surjective deflation morphism

$$\text{Def}_{P/N}^P : Cl_1(\mathbb{Z}P) \rightarrow Cl_1(\mathbb{Z}(P/N)).$$

2.5. Proposition. *Let p be an odd prime and P be a finite p -group. Suppose N is a normal subgroup of P . Let \mathcal{S} be a genetic basis of P and $\mathcal{S}_N = \{S \in \mathcal{S} \mid N \leq S\}$. Let \tilde{B} be the set of subgroups $\tilde{S} = S/N$ of $\tilde{P} = P/N$, for $S \in \mathcal{S}_N$.*

1. *The set $\{\tilde{S} \mid S \in \mathcal{S}_N\}$ is a genetic basis of \tilde{P} , and for $S \in \mathcal{S}_N$, the projection $P \mapsto \tilde{P}$ induces an isomorphism $\pi_S : N_P(S)/S \rightarrow N_{\tilde{P}}(\tilde{S})/\tilde{S}$.*
2. *The composition*

$$s : \Gamma(P) = \prod_{S \in \mathcal{S}} (N_P(S)/S) \longrightarrow \prod_{S \in \mathcal{S}_N} (N_P(S)/S) \xrightarrow{\prod \pi_S} \prod_{\tilde{S} \in \tilde{\mathcal{S}}} (N_{\tilde{P}}(\tilde{S})/\tilde{S}) = \Gamma(\tilde{P})$$

induces a surjective deflation morphism $\text{Def}_{P/N}^P : Cl_1(\mathbb{Z}P) \rightarrow Cl_1(\mathbb{Z}(P/N))$. In particular $Cl_1(\mathbb{Z}(P/N))$ is isomorphic to a quotient of $Cl_1(\mathbb{Z}P)$.

Proof. For Assertion 1, it is clear from the definitions that if S/N is a genetic subgroup of P/N , then S is a genetic subgroup of P . Moreover the irreducible representation of P associated to S is obtained by inflation from P/N to P of the irreducible representation of P/N associated to S/N , up to the obvious isomorphism $\pi_S : N_P(S)/S \cong N_{\tilde{P}}(\tilde{S})/\tilde{S}$.

For Assertion 2, as the map $s : \Gamma(P) \rightarrow \Gamma(\tilde{P})$ is surjective, all we have to check is that the subgroup \mathcal{R} of defining relations for $Cl_1(\mathbb{Z}P) \cong \Gamma(P)/\mathcal{R}$ is mapped by s inside the corresponding subgroup $\tilde{\mathcal{R}}$ of defining relations for $Cl_1(\mathbb{Z}\tilde{P}) \cong \Gamma(\tilde{P})/\tilde{\mathcal{R}}$. So let H be a cyclic subgroup of P , let $g \in C_P(H)$, and let $S \in \mathcal{S}_N$. Then $\tilde{H} = HN/N$ is cyclic, and $\tilde{g} = gN \in C_{\tilde{P}}(\tilde{H})$. Moreover the map

$$H \backslash P/N_P(S) \ni HxN_P(S) \mapsto \tilde{H}\tilde{x}N_{\tilde{P}}(\tilde{S}) \in \tilde{H} \backslash \tilde{P}/N_{\tilde{P}}(\tilde{S}),$$

where $\tilde{x} = xN \in \tilde{P}$, is a bijection, since $HxN_P(S) = HxNN_P(S) = HNxN_P(S)$ as $N_P(S) \geq S \geq N$. Hence we may identify the sets of representatives $[H \backslash P/N_P(S)]$ and $[\tilde{H} \backslash \tilde{P}/N_{\tilde{P}}(\tilde{S})]$ via this map. Moreover

$$H^x \cap N_P(S) \leq S \iff (HN)^x \cap N_P(S) \leq S \iff \tilde{H}^{\tilde{x}} \cap N_{\tilde{P}}(\tilde{S}) \leq \tilde{S}.$$

Now, for $x \in [H \backslash P/N_P(S)]$ such that $H^x \cap N_P(S) \leq S$, the equality $gx = \widetilde{h_{g,x}\sigma_g(x)n_{g,x}}$, where $h_{g,x} \in H$, $\sigma_g(x) \in [H \backslash P/N_P(S)]$, and $n_{g,x} \in N_P(S)$, also reads $\tilde{g}\tilde{x} = \widetilde{h_{g,x}\sigma_g(x)\widetilde{n_{g,x}}}$ in \tilde{P}/N . In other words $\pi_S(\overline{n_{g,x}}) = \overline{\tilde{n}_{\tilde{g},\tilde{x}}}$, that is $s(u_{H,g}) = u_{\tilde{H},\tilde{g}}$. This completes the proof. \square

2.6. Remark. It is shown in [4] (where $\Gamma(P)$ is called the *genome* of P) that the map s is the deflation map in a structure of *biset functor* on Γ , but we will not need the corresponding additional operations of induction, restriction and inflation in this paper.

3. Computing some Whitehead groups

The examples we will consider in this section are all finite p -groups with p odd that satisfy the hypothesis of Theorem 8.10 in [13], so the group $SK_1(\mathbb{Z}P)$ is equal to $Cl_1(\mathbb{Z}P)$. Hence, we will use Theorem 2.4 to calculate $Cl_1(\mathbb{Z}P)$. If P is abelian, Theorem 2.4 has a simpler expression, as it was already noted in Observation 1.13 of [14].

As we said in the introduction, to calculate the free rank of the Whitehead group of the groups in question, we will use Theorem 2.6 in [13]. We will also use Exercise 13.9 in Serre [16], which says that if G is a group of odd order and c is the number of irreducible non-isomorphic complex representations of G , then $(c+1)/2$ is the number of irreducible non-isomorphic real representations of G .

We introduce some notation that will be helpful in both of our examples.

3.1. Notation. *Let p be a prime. Suppose that W is a finite-dimensional vector space over the finite field \mathbb{F}_p . We denote by $S(W)$ the symmetric algebra of W and by $S^p(W)$ its homogeneous part of degree p . If $\psi : W \rightarrow \mathbb{F}_p$ is a linear functional, the map*

$$w_1 \otimes_{\mathbb{F}_p} \dots \otimes_{\mathbb{F}_p} w_n \in W^{\otimes n} \mapsto \psi(w_1) \dots \psi(w_n) \in \mathbb{F}_p$$

induces a well defined linear functional $S(W) \rightarrow \mathbb{F}_p$, that we denote by $A \mapsto A(\psi)$.

The choice of a basis $\{x_1, \dots, x_k\}$ of W over \mathbb{F}_p yields a standard identification of $S(W)$ with the polynomial ring $\mathbb{F}_p[x_1, \dots, x_k]$.

With such an identification, if $A = A(x_1, \dots, x_k) \in S(W)$ and ψ is a linear form on W , then $A(\psi) = A(\psi(x_1), \dots, \psi(x_k))$. In particular $A(\psi) = 0$ for all ψ if and only if the polynomial function associated to A is equal to zero, that is if $A(r_1, \dots, r_k) = 0$ for any $(r_1, \dots, r_k) \in \mathbb{F}_p^k$: indeed since $\{x_1, \dots, x_k\}$ is a basis of W , for any such k -tuple $(r_1, \dots, r_k) \in \mathbb{F}_p^k$, there is a unique linear form ψ on W such that $\psi(x_i) = r_i$ for $1 \leq i \leq k$.

3.2. Elementary abelian p -groups.

3.3. Lemma. *Let p be an odd prime and P be an elementary abelian p -group of rank k , the free rank of $Wh(P)$ is equal to*

$$\frac{(p^k - 1)(p - 3)}{2(p - 1)}.$$

Proof. The number of non-isomorphic irreducible \mathbb{R} -representations of P is $(p^k + 1)/2$. On the other hand, the number of non-isomorphic irreducible \mathbb{Q} -representations of P

is equal to $(p^k + p - 2)/(p - 1)$, since the genetic basis for P is given by all its subgroups of index p plus P itself. The result follows from Theorem 2.6 in [13]. \square

The description of SK_1 for elementary abelian groups appeared first in Alperin et al. [1], we prove this result now using genetic bases. Our proof has some similarities with the one appearing in [1], but it is a bit simpler, thanks to the use of genetic bases. The proof will also be useful when dealing with extra-special p -groups.

3.4. Lemma. *Let p be a prime and let W be a finite-dimensional vector space over \mathbb{F}_p . For x and y in W , we set $B_{x,y} = x^{p-1}y \in S^p(W)$. Then $S^p(W)$ is generated by the elements $B_{x,y}$ with x and y running over W .*

Proof. Recall that if x_1, \dots, x_m are m (not necessarily different) commuting variables, then for any n

$$(x_1 + \dots + x_m)^n = \sum_{\substack{\alpha_1, \dots, \alpha_m \text{ s.t.} \\ \alpha_1 + \dots + \alpha_m = n}} \frac{n!}{\alpha_1! \dots \alpha_m!} x_1^{\alpha_1} \dots x_m^{\alpha_m}.$$

This allows us to show that for any n

$$(3.5) \quad \sum_{\emptyset \neq A \subseteq \{1, \dots, n\}} (-1)^{n-|A|} \left(\sum_{i \in A} x_i \right)^n = n! x_1 \dots x_n,$$

and so if p is prime, then

$$\sum_{\emptyset \neq A \subseteq \{1, \dots, p-1\}} (-1)^{p-1-|A|} \left(\sum_{i \in A} x_i \right)^{p-1} x_p = (p-1)! x_1 \dots x_p,$$

which by Wilson's Lemma gives

$$\sum_{\emptyset \neq A \subseteq \{1, \dots, p-1\}} (-1)^{p-1-|A|} \left(\sum_{i \in A} x_i \right)^{p-1} x_p = x_1 \dots x_p,$$

that is

$$(3.6) \quad \sum_{\emptyset \neq A \subseteq \{1, \dots, p-1\}} (-1)^{p-1-|A|} B_{\sum_{i \in A} x_i, x_p} = x_1 \dots x_p.$$

This completes the proof, by taking $x_1, \dots, x_p \in W = S^1(W)$, which indeed commute in $S(W)$. \square

3.7. Theorem. *[Theorem 2.4 in [1]] Let p be an odd prime and P be an elementary abelian p -group of rank k , then $SK_1(\mathbb{Z}P)$ is isomorphic to $(C_p)^N$ where*

$$N = \frac{p^k - 1}{p - 1} - \binom{p + k - 1}{p}.$$

Proof. As we said before, the genetic basis of P consists of P itself and all its subgroups of index p , so $SK_1(\mathbb{Z}P)$ is isomorphic to the quotient of

$$\Gamma(P) = \prod_{[P:Q]=p} (P/Q)$$

by the subgroup generated by the elements $u_{x,y}$ for x, y in P , where

$$(u_{x,y})_Q = \begin{cases} yQ & \text{if } x \in Q \\ 1 & \text{otherwise.} \end{cases}$$

On the other hand, we can see P as a vector space over \mathbb{F}_p , and for each subgroup Q of index p , i.e. for each hyperplane Q of P , consider $\psi_Q : P \rightarrow \mathbb{F}_p$, a linear functional with kernel Q . The product of these ψ_Q induces an isomorphism from $\Gamma(P)$ to

$$V = \prod_{[P:Q]=p} \mathbb{F}_p,$$

and the elements $u_{x,y}$ can be seen as

$$(u_{x,y})_Q = \begin{cases} \psi_Q(y) & \text{if } x \in Q \\ 0 & \text{otherwise.} \end{cases}$$

We define a morphism $r : S^p(P) \rightarrow V$, sending $A \in S^p(P)$ to the vector whose Q -component is equal to $A(\psi_Q)$. We will show that $\text{Im}(r)$ is equal to the subspace of V generated by the elements $u_{x,y}$, and that r is injective. This will give us the result.

We show first that the elements $u_{x,y}$ are in $\text{Im}(r)$. For $x, y \in P$, let $B_{x,y} = x^{p-1}y \in S^p(P)$. Then

$$B_{x,y}(\psi_Q) = \psi_Q(x)^{p-1}\psi_Q(y) = \begin{cases} 0 & \text{if } x \in Q \\ \psi_Q(y) & \text{otherwise} \end{cases}$$

since $\lambda^{p-1} = 1$ if λ is in $\mathbb{F}_p - \{0\}$ and $0^{p-1} = 0$. In particular $B_{y,y}(\psi_Q) = \psi_Q(y)$ for all $y \in P$, thus $r(B_{y,y} - B_{x,y}) = u_{x,y}$.

On the other hand, by Lemma 3.4, $S^p(P)$ is generated by the elements $B_{x,y}$ where x and y run through P , so we have that $\text{Im}(r)$ is contained in (hence equal to) the subspace of V generated by the elements $u_{x,y}$.

Finally, we prove that r is injective. Let A be in the kernel of r , then $A(\psi_Q) = 0$ for every Q of index p in P . If ψ is any other linear functional of P with kernel Q , then there exists $\lambda \in \mathbb{F}_p$ such that $\psi = \lambda\psi_Q$, and so $A(\psi) = \lambda^p A(\psi_Q) = 0$, since A is homogeneous of degree p . Choosing a basis of P over \mathbb{F}_p as in Notation 3.1, we can view A as a homogeneous polynomial of degree p , and the polynomial function A is zero. It remains to see that A is actually the zero polynomial, but this will be clear after the following lemma. \square

3.8. Lemma. *Let \mathbb{F} be a field of characteristic $p > 0$ and k be a positive integer. Let A be a homogeneous polynomial of degree $d \leq p$ in k variables x_1, \dots, x_k . If $A(x_1, \dots, x_k) = 0_{\mathbb{F}}$ for all $(x_1, \dots, x_k) \in \mathbb{F}^k$, then $A = 0$.*

Proof. We proceed by induction on k . If $k = 1$, then A is of the form $A(x_1) = ax_1^d$, for some $a \in \mathbb{F}$. Hence $A(1_{\mathbb{F}}) = 0_{\mathbb{F}} = a$, and A is the zero polynomial, starting induction.

Assume the results holds for homogeneous polynomials of degree $d \leq p$ in less than k variables. Write

$$A(x_1, \dots, x_k) = A_d(x_2, \dots, x_k)x_1^d + A_{d-1}(x_2, \dots, x_k)x_1^{d-1} + \dots + A_0(x_2, \dots, x_k),$$

where $A_i(x_2, \dots, x_k)$ is either the zero polynomial or a homogeneous polynomial of degree $d - i$ in x_2, \dots, x_k , for $0 \leq i \leq d$.

Let $v = (x_2, \dots, x_k)$ be an element in \mathbb{F}^{k-1} . For each $i \in \{0, \dots, d\}$, set $a_i = A_i(x_2, \dots, x_k)$. Then the polynomial

$$P_v(x_1) = a_d x_1^d + a_{d-1} x_1^{d-1} + \dots + a_0$$

vanishes for all $x_1 \in \mathbb{F}_p \subseteq \mathbb{F}$. If $d < p$, then P_v must be the zero polynomial, because otherwise it would have more than d different roots. It follows that $a_i = 0_{\mathbb{F}}$ for $0 \leq i \leq d$. Since this argument holds for any $v \in \mathbb{F}^{k-1}$, we have $A_i(x_2, \dots, x_k) = 0_{\mathbb{F}}$ for any $v = (x_2, \dots, x_k) \in \mathbb{F}^{k-1}$. If $A_i \neq 0$ for some $i \in \{0, \dots, d\}$, then A_i is homogeneous of degree $d - i \leq p$, and it follows by induction that $A_i = 0$ for $0 \leq i \leq d$, contradicting the assumption. Hence $A_i = 0$ for $0 \leq i \leq d$, so $A = 0$.

Now if $d = p$, then there exists $\lambda = \lambda(x_2, \dots, x_k) \in \mathbb{F}$ such that

$$a_p x_1^p + a_{p-1} x_1^{p-1} + \dots + a_0 = \lambda(x_1^p - x_1).$$

Hence $a_i = 0_{\mathbb{F}} = A_i(x_2, \dots, x_k)$ for $i = 0$ and for $2 \leq i \leq p-1$. Since this holds for any $(x_2, \dots, x_k) \in \mathbb{F}^{k-1}$, by induction we have $A_i = 0$ for $i = 0$ and for $2 \leq i \leq p-1$. Finally

$a_1 = -\lambda = A_1(x_2, \dots, x_k)$ and $a_p = \lambda = A_p(x_2, \dots, x_k)$ for any $(x_2, \dots, x_k) \in \mathbb{F}^{k-1}$, that is

$$A_1(x_2, \dots, x_k) = -A_p(x_2, \dots, x_k).$$

But A_p is homogeneous of degree 0, i.e. it is a constant polynomial. Taking $x_2 = x_3 = \dots = x_k = 0_{\mathbb{F}}$ in the previous equality, we get

$$A_1(0_{\mathbb{F}}, \dots, 0_{\mathbb{F}}) = 0_{\mathbb{F}} = A_p(0_{\mathbb{F}}, \dots, 0_{\mathbb{F}}),$$

where the first equality holds because A_1 is homogeneous of degree $p-1 > 0$. It follows that $A_p = 0$, and now $A_1(x_2, \dots, x_k) = 0_{\mathbb{F}}$ for any $(x_2, \dots, x_k) \in \mathbb{F}^{k-1}$. By induction $A_1 = 0$, hence $A = 0$. \square

3.9. Corollary. *Let p be an odd prime, and P be a finite p -group. If $|P/\Phi(P)| = p^k$, then $SK_1(\mathbb{Z}P)$ has a subquotient isomorphic to $(C_p)^N$, where*

$$N = \frac{p^k - 1}{p - 1} - \binom{p + k - 1}{p},$$

and in particular $SK_1(\mathbb{Z}P) \neq 0$ if $k \geq 3$.

Proof. Indeed $Cl_1(\mathbb{Z}(P/\Phi(P))) \cong (C_p)^N$, for $N = \frac{p^k - 1}{p - 1} - \binom{p + k - 1}{p}$, by Theorem 3.7. Moreover, this group is a quotient of $Cl_1(\mathbb{Z}P)$, by Proposition 2.5. Finally $Cl_1(\mathbb{Z}P)$ is a subgroup of $SK_1(\mathbb{Z}P)$, and $N > 0$ if $k \geq 3$. \square

3.10. Extra-special and almost extra-special p -groups.

We begin by finding a genetic basis of an (almost) extra-special p -group.

3.11. Proposition. *Let p be a prime and P be an (almost) extra-special p -group. A genetic basis of P is given by all its subgroups of index p , together with P and a subgroup Y of maximal order such that $Y \cap Z(P) = 1$. In particular P has a unique faithful rational irreducible representation, up to isomorphism.*

Proof. We abbreviate $Z(P)$ by Z .

By theorems 1.7 and 1.8, the subgroups of P of index 1 or p are genetic and are not linked modulo \trianglelefteq_P . They clearly intersect Z non-trivially. On the other hand, any genetic subgroup $S \neq P$ which intersects Z non-trivially must have index p , since $P' \leq S$ and so the cyclic group $P/S \cong (P/P')/(S/P')$, should have order p . This implies that if there is another group in \mathcal{S} , it must intersect Z trivially.

Let $Y \leq P$ be of maximal order with the property $Y \cap Z = \mathbf{1}$. By Lemma 1.18, we have that $C_P(Y) = N_P(Y) = YZ$. In particular $N_P(Y) \trianglelefteq P$ and $N_P(Y)/Y \cong Z$ is a Roquette group. Then Y is genetic, by Remark 1.12. Also, by Lemma 1.18, we have that if $Y_1 \leq P$ is a group such that $Y_1 \cap Z = \mathbf{1}$, but it is not maximal order with this property, then $C_P(Y_1) = N_P(Y_1)$, but $N_P(Y_1)/Y_1$ is not cyclic. Thus Y_1 is not a genetic subgroup of P .

Finally, if Y is a subgroup of P of maximal order such that $Y \cap Z = \mathbf{1}$, then Y has $|P/YZ| = |Y|$ distinct conjugates in P , by Lemma 1.18. These conjugates are subgroups of index p in the elementary abelian group YP' , and they all intersect trivially (that is, they don't contain) the group P' . Since there are exactly $|Y|$ subgroups of YP' not containing P' , these subgroups are exactly the conjugates of Y in P .

Now if Y_0 is another subgroup of P such that $Y_0 \cap Z = \mathbf{1}$, then $Y_0 \cap YP'$ is a subgroup of YP' which does not contain P' . Hence it is contained in some conjugate of Y , and there exists $x \in P$ such that $Y_0 \cap YP' \leq Y^x$. It follows that $Y_0 \cap YZ \leq Y^x$, for YP' is the subgroup of YZ consisting of elements of order at most p . In other words

$${}^xY_0 \cap Z_P(Y) = {}^xY_0 \cap YZ = {}^x(Y_0 \cap YZ) \leq Y.$$

Now if Y_0 is another subgroup of maximal order such that $Y_0 \cap Z = \mathbf{1}$, exchanging the roles of Y and Y_0 in the previous argument shows that there also exists an element $y \in P$ such that ${}^yY \cap Y_0Z \leq Y_0$. By Theorem 1.8, it follows that $Y_0 \trianglelefteq_P Y$. The last assertion now follows from Lemma 1.10. \square

As a first consequence of this result we have.

3.12. Lemma. *Let p be an odd prime, and n be a positive integer.*

1. *Let P be an extra-special p -group of order p^{2n+1} . Then the free rank of $Wh(P)$ is equal to*

$$\frac{(p^{2n} + p - 2)(p - 3)}{2(p - 1)}.$$

2. *Let P be an almost extra-special group of order p^{2n+2} . Then the free rank of $Wh(P)$ is equal to*

$$\frac{(p^{2n+1} + p^2 + p + 1)(p - 3) + 8}{2(p - 1)}.$$

Proof. The free rank of $Wh(P)$ is equal to $r - q$, where r (resp. q) is the number of irreducible real (resp. rational) representations of P , up to isomorphism. In general, for a finite p -group P and a field K of characteristic 0, the irreducible representations

of P over K can be recovered from the knowledge of a genetic basis \mathcal{B} of P (see [2]): this is because the functor R_K of representations of p -groups over K is *rational* in the sense of Definition 10.1.3 of [5], as can be easily deduced from Theorem 10.6.1 of [5]. A proof of this fact can also be found in [6]. In particular, the number $l_K(P)$ of such representations, up to isomorphism, is equal to

$$l_K(P) = \sum_{S \in \mathcal{B}} \partial l_K(N_P(S)/S),$$

where $\partial l_K(Q)$ denotes the number of *faithful* irreducible representations of a p -group Q over K , up to isomorphism. For a Roquette p -group Q , we have moreover $\partial l_K(Q) = 1$ if $Q = \mathbf{1}$, and $\partial l_K(Q) = l_K(Q) - l_K(Q/Z)$ otherwise, where Z is the unique central subgroup of order p of Q .

If p is odd, all the groups $N_P(S)/S$, for $S \in \mathcal{B}$, are cyclic. Now for $Q = C_{p^m}$, with $m \geq 0$, we have

$$l_{\mathbb{R}}(Q) = \frac{p^m + 1}{2} \quad \text{and} \quad l_{\mathbb{Q}}(Q) = m + 1.$$

It follows that $\partial l_{\mathbb{R}}(Q) = \frac{p^m - p^{m-1}}{2}$ if $m > 0$, and $\partial l_{\mathbb{R}}(Q) = 1$ if $m = 0$. On the other hand $\partial l_{\mathbb{Q}}(Q) = 1$ for any m .

In case P is extra-special of order p^{2n+1} , the genetic basis obtained in Proposition 3.11 consists of the group $S = P$, for which $N_P(S)/S$ is trivial, of $\frac{p^{2n}-1}{p-1}$ subgroups S of index p in P , for which $N_P(S)/S \cong C_p$, and the subgroup $S = Y$, for which $N_P(S)/S \cong Z(P) \cong C_p$. This gives

$$r = l_{\mathbb{R}}(P) = 1 + \frac{p^{2n}-1}{p-1} \frac{p-1}{2} + \frac{p-1}{2} = \frac{p^{2n}+p}{2},$$

and

$$q = l_{\mathbb{Q}}(P) = 1 + \frac{p^{2n}-1}{p-1} + 1 = \frac{p^{2n}+2p-3}{p-1}.$$

In case P is almost extra-special of order p^{2n+2} , the genetic basis obtained in Proposition 3.11 consists of the group $S = P$, for which $N_P(S)/S$ is trivial, of $\frac{p^{2n+1}-1}{p-1}$ subgroups S of index p in P , for which $N_P(S)/S \cong C_p$, and the subgroup $S = Y$, for which $N_P(S)/S \cong Z(P) \cong C_{p^2}$. This gives

$$r = l_{\mathbb{R}}(P) = 1 + \frac{p^{2n+1}-1}{p-1} \frac{p-1}{2} + \frac{p^2-p}{2} = \frac{p^{2n+1}+p^2-p+1}{2},$$

and

$$q = l_{\mathbb{Q}}(P) = 1 + \frac{p^{2n+1}-1}{p-1} + 1 = \frac{p^{2n+1}+2p-3}{p-1}.$$

This completes the proof. □

To calculate $Cl_1(\mathbb{Z}P)$ we will need the following result.

3.13. Lemma. *Let p be an odd prime. Let W be a vector space over \mathbb{F}_p of finite dimension k , which is endowed with a bilinear, alternating form $b : W \times W \rightarrow \mathbb{F}_p$. Suppose that the rank of b is not equal to 2.*

For x and y in W , we still set $B_{x,y} = x^{p-1}y \in S^p(W)$. Then we have

$$S^p(W) = \langle B_{x,y} \mid x, y \in W \text{ s.t. } b(x, y) = 0 \rangle.$$

Proof. We will write \mathcal{O} for $\langle B_{x,y} \mid x, y \in W \text{ s.t. } b(x, y) = 0 \rangle$. We will prove that $B_{x,y} \in \mathcal{O}$ for any $x, y \in W$, and by Lemma 3.4, it will follow that $S^p(W) = \mathcal{O}$.

Observe that, since $B_{x,y} \in \mathcal{O}$ for an $x, y \in W$ with $b(x, y) = 0$, it follows from formula 3.6 that $x_1 x_2 \dots x_{p-1} y \in \mathcal{O}$ for any elements x_1, \dots, x_{p-1} of W such that $b(x_i, y) = 0$ for $1 \leq i \leq p-1$.

If $b = 0$, there is nothing to prove. Otherwise let $x, y \in W$ such that $b(x, y) \neq 0$. Since $B_{x,\lambda y} = \lambda B_{x,y}$ for $\lambda \in \mathbb{F}_p$, to prove that $B_{x,y} \in \mathcal{O}$, we can assume without loss of generality that $b(x, y) = 1$, up to replacing y by a suitable scalar multiple. If the restriction of b to $\langle x, y \rangle^\perp$ was identically 0, then $\langle x, y \rangle^\perp$ would be precisely the radical of b , so b would have rank 2, contradicting our assumption. Hence we can find $z, t \in \langle x, y \rangle^\perp$ such that $b(z, t) \neq 0$, and up to replacing t by some scalar multiple, we can assume that $b(z, t) = 1$.

Now let $\alpha \in \mathbb{F}_p$, and set $u = \alpha x + t$ and $v = y + \alpha z$. Then

$$b(u, v) = \alpha b(x, y) + \alpha^2 b(x, z) + b(t, y) + \alpha b(t, z) = 0,$$

since $b(x, y) = 1 = -b(t, z)$ and $b(x, z) = 0 = b(t, y)$.

It follows that $B_{u,v} \in \mathcal{O}$. But $B_{u,v}$ is equal to

$$(3.14) \quad (\alpha x + t)^{p-1}(y + \alpha z) = \sum_{i=0}^{p-1} \binom{p-1}{i} \alpha^i x^i y t^{p-1-i} + \sum_{i=0}^{p-1} \binom{p-1}{i} \alpha^{i+1} t^{p-1-i} z x^i.$$

By the observation at the beginning of the proof, the element $x^i y t^{p-1-i}$ is in \mathcal{O} whenever $p-1-i > 0$, since $b(x, t) = b(y, t) = b(t, t) = 0$. Similarly $t^{p-1-i} z x^i \in \mathcal{O}$ if $i > 0$, since $b(t, x) = b(z, x) = b(x, x) = 0$. It follows that in (3.14), the only elements possibly not in \mathcal{O} correspond to $p-1-i = 0$ in the first summation and to $i = 0$ in the second. Hence

$$\alpha^{p-1} x^{p-1} y + \alpha t^{p-1} z \in \mathcal{O},$$

and this holds for any $\alpha \in \mathbb{F}_p$. For $\alpha = 1$, this gives $x^{p-1} y + t^{p-1} z \in \mathcal{O}$, and for $\alpha = -1$, this gives $x^{p-1} y - t^{p-1} z \in \mathcal{O}$. It follows that $x^{p-1} y \in \mathcal{O}$, as was to be shown. \square

3.15. Remark. If the rank of b is equal to 2, then the result of Lemma 3.13 is no longer true: for example in the non-degenerate case, that is when W has dimension 2, saying that $b(x, y) = 0$ for $x \neq 0$ is equivalent to saying that y is a scalar multiple of x . In this case \mathcal{O} is the subspace of $S^p(W)$ generated by the elements x^p , for $x \in W$. So \mathcal{O} has dimension 2, whereas $S^p(W)$ has dimension $p + 1$.

We now come to our main theorem, describing the structure of $Cl_1(\mathbb{Z}P)$ when P is an extra-special or almost extra-special p -group for p odd. We first recall that Oliver ([13] Example 7 page 16) showed that if P is extra-special of order p^3 , then $Cl_1(\mathbb{Z}P) \cong (C_p)^{p-1}$, and that if P is almost extra-special of order p^4 , then $Cl_1(\mathbb{Z}P) \cong (C_p)^{(p^2+p-2)/2}$. Hence it what follows, we may assume that P is an extra-special group of order at least p^5 , or an almost extra-special p -group of order at least p^6 .

3.16. Notation. Let p be an odd prime and n be a positive integer. Let P be an extra-special p -group of order p^{2n+1} or an almost extra-special p -group of order p^{2n+2} . Let Z denote the center of P , and $N = P' \leq Z$ be the Frattini subgroup of P . Let Y be a subgroup of P of maximal order such that $Y \cap Z = \mathbf{1}$, as in Proposition 3.11. Recall that Y is elementary abelian. In any case, the group P can be written as a semidirect product $P = X \cdot Y$, where $X \geq Z$ is an abelian normal subgroup of P with $Y \cap X = \mathbf{1}$:

- If P is extra-special of exponent p , the group X is equal to $C \times X_0$, for some subgroup $X_0 \cong (C_p)^n$ and $C = N = Z$.
- If P is extra-special of exponent p^2 , the group X is equal to $C \times X_0$, for some subgroup $X_0 \cong (C_p)^{n-1}$, some subgroup $C \cong C_{p^2}$, and $N = Z < C$.
- If P is almost extra-special, then $X = C \times X_0$, for some subgroup $X_0 \cong (C_p)^n$, and $N < Z = C \cong C_{p^2}$.

So in all cases we have $X = C \times X_0$, for some cyclic subgroup $C \geq Z \geq N$.

Moreover the subgroup Y is elementary abelian of order p^n . It is maximal subject to the condition $Y \cap Z = \mathbf{1}$, so by Proposition 3.11, we have a genetic basis of P consisting of P itself, its subgroups of index p , and Y . The normalizer $N_P(Y)$ is equal to $Z \cdot Y$, so

$$\Gamma(P) \cong \left(\prod_{[P:Q]=p} (P/Q) \right) \times Z.$$

We will often use an additive notation for $\Gamma(P)$ and its components.

3.17. Theorem. *Let p be an odd prime, and let P be an extra-special p -group of order at least p^5 , or an almost extra-special p -group of order at least p^6 . Let $N = P'$ be the*

Frattini subgroup of P , and Z be the center of P . Then there is a split sequence of abelian groups

$$0 \longrightarrow K \longrightarrow Cl_1(\mathbb{Z}P) \xrightarrow{\text{Def}_{P/N}^P} Cl_1(\mathbb{Z}(P/N)) \longrightarrow 0,$$

where K is cyclic, generated by the image in $Cl_1(\mathbb{Z}P)$ of the unique faithful rational irreducible representation of P . Moreover K is isomorphic to the quotient of Z by the subgroup generated by all the elements $u_{H,g,Y} \in N_P(Y)/Y \cong Z$ introduced in Theorem 2.4, where H is a cyclic subgroup of P and $g \in C_P(H)$.

Proof. The product $\prod_{[P:Q]=p} (P/Q)$ identifies with $\Gamma(P/N)$, and we have a surjective projection map $\text{Def}_{P/N}^P : \Gamma(P) \rightarrow \Gamma(P/N)$, with kernel isomorphic to Z . By Proposition 2.5, this map induces a surjective deflation map

$$\text{Def}_{P/N}^P : Cl_1(\mathbb{Z}P) = \Gamma(P)/\mathcal{R} \rightarrow Cl_1(\mathbb{Z}(P/N)) = \Gamma(P/N)/\overline{\mathcal{R}},$$

where \mathcal{R} is the subgroup of $\Gamma(P)$ generated by the elements $u_{H,g}$ introduced in Theorem 2.4, and H is a cyclic subgroup of P with $g \in C_P(H)$. Similarly $\overline{\mathcal{R}}$ is the corresponding subgroup of $\Gamma(P/N)$ generated by the elements $u_{F,c}$, where F is a cyclic subgroup of P/N and $c \in P/N$ (we always have $c \in C_{P/N}(F)$, as P/N is abelian).

The proof of Theorem 2.5 shows that $\text{Def}_{P/N}^P(u_{H,g}) = u_{HN/N,gN}$. Conversely, if F is a cyclic subgroup of P/N , generated by f , and if $c \in P/N$, then there exists a pair (H, g) of a cyclic subgroup H of P and an element $g \in C_P(H)$ such that $HN/N = F$ and $gN = c$ if and only if $b(f, c) = 0$, where b is the bilinear alternating form on P/N with values in \mathbb{F}_p induced by taking commutators in P . Our assumptions on P imply that the rank of b is not 2, so we can apply Lemma 3.13. This shows that the subspace of $\Gamma(P/N)$ generated by the elements $u_{F,c}$, where $F = \langle f \rangle$ for $f \in P/N$, and $c \in P/N$ such that $b(f, c) = 0$, generate $S^p(P/N) = \overline{\mathcal{R}}$, by Lemma 3.4. It follows that $\text{Def}_{P/N}^P$ induces a surjective map $\mathcal{R} \rightarrow \overline{\mathcal{R}}$. Let L denote the kernel of this map. We have a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & L & \longrightarrow & \mathcal{R} & \xrightarrow{\text{Def}_{P/N}^P} & \overline{\mathcal{R}} \longrightarrow 0 \\ & & \downarrow l & & \downarrow i & & \downarrow j \\ 0 & \longrightarrow & Z & \longrightarrow & \Gamma(P) & \xrightarrow{\text{Def}_{P/N}^P} & \Gamma(P/N) \longrightarrow 0 \end{array}$$

where the vertical maps i and j are the inclusion maps. The Snake's Lemma now shows that the map l is injective, and moreover we have an exact sequence of cokernels

$$(3.18) \quad 0 \longrightarrow K \longrightarrow Cl_1(\mathbb{Z}P) \xrightarrow{\text{Def}_{P/N}^P} Cl_1(\mathbb{Z}(P/N)) \longrightarrow 0,$$

where $K = Z/l(L)$. Since the kernel Z of $\text{Def}_{P/N}^P$ corresponds to the component of $\Gamma(P)$ indexed by Y , the image $l(L)$ is generated by the components $u_{H,g,Y} \in N_P(Y)/Y \cong Z$, where H is a cyclic subgroup of P and $g \in C_P(H)$.

It remains to see that the exact sequence 3.18 splits. To see this, consider the completed diagram

$$\begin{array}{ccccccc}
& 0 & & 0 & & 0 & \\
& \downarrow & & \downarrow & & \downarrow & \\
0 & \longrightarrow & L & \longrightarrow & \mathcal{R} & \longrightarrow & \overline{\mathcal{R}} \longrightarrow 0 \\
& & \downarrow l & & \downarrow i & & \downarrow j \\
0 & \longrightarrow & Z & \longrightarrow & \Gamma(P) & \xrightarrow{c} & \Gamma(P/N) \longrightarrow 0 \\
& & \downarrow & & \downarrow a & \swarrow \text{---} t \text{---} & \downarrow \begin{smallmatrix} s \downarrow \\ b \end{smallmatrix} \\
0 & \longrightarrow & K & \longrightarrow & Cl_1(\mathbb{Z}P) & \xrightarrow{d} & Cl_1(\mathbb{Z}(P/N)) \longrightarrow 0, \\
& & \downarrow & & \downarrow & & \downarrow \\
& & 0 & & 0 & & 0
\end{array}$$

where a and b are the projection maps, and c , d are the respective deflation maps. The map b is split surjective, because $\Gamma(P/N)$ and $Cl_1(\mathbb{Z}(P/N))$ are both elementary abelian. Let s be a section of b . Similarly, the map c is split surjective by construction. Let $t : \Gamma(P/N) \rightarrow \Gamma(P)$ be a section of c . Then

$$d \circ a \circ t \circ s = b \circ c \circ t \circ s = b \circ s = \text{Id},$$

so the map $a \circ t \circ s$ is a section of d . This completes the proof. \square

So to go further, we have to focus on the computation of the elements $u_{H,g,Y}$ appearing in Theorem 3.17. First a technical lemma:

3.19. Lemma. *Keeping Notation 3.16, let H be a cyclic subgroup of P . Then there exists a set D (possibly empty) of representatives of those double cosets $HxN_P(Y)$ in P for which $H^x \cap N_P(Y) \leq Y$, and a subgroup X_1 of X_0 of index at most p , such that $DX_1 = D$.*

Proof. If there is no element $x \in P$ such that $H^x \cap N_P(Y) \leq Y$, then we take $D = \emptyset$ and $X_1 = X_0$. So assume that $H^x \cap N_P(Y) \leq Y$ for some $x \in P$.

Since the derived group $P' = N$ is central in P , by standard formulae (see e.g. [10], Chapter 2, Lemma 2.2), for any two elements $a, b \in P$ and any integer m , we

have $(ab)^m = a^m b^m [b, a]^{\binom{m}{2}}$. Suppose that H is generated by $h = \xi\eta$, with $\xi \in X$ and $\eta \in Y$. We can write further $\xi = \gamma\xi_0$, for $\gamma \in C$ and $\xi_0 \in X_0$. We have $H^x \cap N_P(Y) = (H \cap ZY)^x \leq Y$. But $h^p = \xi^p \eta^p [\xi, \eta]^{\binom{p}{2}} = \xi^p = \gamma^p$ since P' , X_0 and Y are elementary abelian and $\binom{p}{2}$ is a multiple of p . Moreover $\gamma \in C$, hence $\gamma^p \in Z$, as Z has index 1 or p in C . Thus $\gamma^p \in H \cap Z = (H \cap Z)^x \leq (H \cap ZY)^x \leq Y$. It follows that $\gamma^p = 1$, and $\gamma \in N \leq Z$. Moreover $h^p = 1$.

If $h = 1$, then $H \backslash P / N_P(Y) = XY / ZY \cong X / Z = (C / Z) \times X_0$, so we can take $D = E \times X_0$, for a chosen set $E = [C / Z]$ of Z -cosets in C , and $X_1 = X_0$. Hence we can assume that h has order p , that is $|H| = p$.

Then there are two cases:

Case 1: Suppose that $H \cap N_P(Y) = 1$, or equivalently $H \not\leq ZY$. Then $H^g \not\leq ZY$, for any $g \in P$, so $H^g \cap ZY = 1 \leq Y$. In this case, we take a subgroup X_1 of X_0 such that $X_0 = \langle \xi_0 \rangle \times X_1$. Observe that X_1 has index at most p in X_0 . We take moreover a set $E = [C / Z]$ of representatives of the cosets C / Z . We claim that the set $D = EX_1$ has the required properties. Since obviously $DX_1 = D$, all we have to show is that D is indeed a set of representatives of $(H, N_P(Y))$ -double cosets in P .

So let $e, e' \in E$ and $x_1, x'_1 \in X_1$, and assume that there exists an integer m , an element $z \in Z$ and an element $y \in Y$, such that

$$e'x'_1 = (h^m)ex_1(zy).$$

Since $h = \gamma\xi_0\eta$, this also reads

$$\begin{aligned} e'x'_1 &= (\gamma\xi_0\eta)^m ex_1(zy) = (\gamma\xi_0)^m \eta^m [\eta, \gamma\xi_0]^{\binom{m}{2}} ex_1 zy \\ &= \gamma^m \xi_0^m [\eta, \gamma\xi_0]^{\binom{m}{2}} ex_1 \eta^m [\eta^m, ex_1] zy \\ e'x'_1 &= \underbrace{\left(\gamma^m [\eta, \gamma\xi_0]^{\binom{m}{2}} e [\eta^m, ex_1] z \right)}_{\in C} x_1 (\eta^m y). \end{aligned}$$

The left hand side is in X . The terms on the right hand side are all in X , except $\eta^m y$, which is in Y . Hence $\eta^m y = 1$, and

$$e'x'_1 = \underbrace{\left(\gamma^m [\eta, \gamma\xi_0]^{\binom{m}{2}} e [\eta^m, ex_1] z \right)}_{\in C} x_1.$$

Since $e' \in C$, $x'_1 \in X_0$, $x_1 \in X_0$, and since $X = C \times X_0$, it follows that $x'_1 = x_1$ and $e' = \left(\gamma^m [\eta, \gamma\xi_0]^{\binom{m}{2}} e [\eta^m, ex_1] z \right)$. Since $\gamma \in Z$, this in turn implies $e' \in eZ$, hence $e' = e$. So the double cosets $HdN_P(Y)$, for $d \in D = EX_1$, are all distinct.

It remains to show that any $(H, N_P(Y))$ -double coset in P is of this form. So let $g \in P = (C \times \langle \xi_0 \rangle \times X_1) \cdot Y$. Hence there exist $c \in C$, $m \in \mathbb{N}$, $x_1 \in X_1$, and $y \in Y$ such that $g = c\xi_0^m x_1 y$. There also exists $e \in E$ and $z' \in Z$ such that $c = ez'$. It follows that

$$\begin{aligned} HgN_P(Y) = HgZY &= Hc\xi_0^m x_1 yZY = Hc\xi_0^m x_1 ZY \\ &= Hc(\xi_0\eta)^m [\eta, \xi_0]^{-\binom{m}{2}} \eta^{-m} x_1 ZY \\ &= Hch^m \eta^{-m} x_1 ZY = Hcx_1 \eta^{-m} [\eta^{-m}, x_1] ZY \\ &= Hcx_1 ZY = Hez'x_1 ZY = Hex_1 ZY, \end{aligned}$$

as was to be shown, since $ex_1 \in D$.

Case 2: Suppose now that $H \leq ZY$ and $H^x \leq Y$. If D is a set of representatives of the (H^x, ZY) -double cosets in P , then xD is a set of representatives of the (H, ZY) -double cosets in P . So without loss of generality, we can assume that $x = 1$, that is $H \leq Y$. If $g \in G$, then $HgZY = HZYg = ZYg = gZY$, so $H \backslash P / ZY = P / ZY$. If moreover $H^g \leq Y$, then as $h^g = h[h, g]$, we have $[h, g] \in Z \cap Y = \mathbf{1}$, and $g \in C_P(H)$. Hence we seek for a set D of representatives of $C_P(H)/ZY$. But $Y \leq C_P(H) \leq XY$, so $C_P(H) = C_X(H)Y$, hence $C_P(H)/ZY \cong C_X(H)/Z$.

Now $C_P(H)$ is a subgroup of index p of P , by Lemma 1.18, since H has order p and H is not central in P . Hence $C_X(H)$ has index p in $X = C \times X_0$. So the group $X_1 = C_{X_0}(H)$ has index at most p in X_0 , and moreover there exists a subgroup $X_2 \geq Z$ of $C_X(H)$ such that $C_X(H) = X_2 \times X_1$. Choosing a set E of representatives of X_2/Z , the set $D = EX_1$ is a set of representatives of $C_X(H)/Z$ with the required properties.

This completes the proof. \square

3.20. Theorem. *Let p be an odd prime, and let P be an extra-special p -group of order at least p^5 or an almost extra-special p -group of order at least p^6 . Set $N = \Phi(P) = P'$.*

1. *The group $Cl_1(\mathbb{Z}P)$ is isomorphic to $K \times (C_p)^M$, where $M = \frac{p^{k-1}-1}{p-1} - \binom{p+k-2}{p}$ if $|P| = p^k$, and K is the kernel of $\text{Def}_{P/N}^P : Cl_1(\mathbb{Z}P) \rightarrow Cl_1(\mathbb{Z}(P/N))$.*
2. *Moreover, the group K is:*
 - (a) *trivial if P is extra-special of order p^5 and exponent p^2 .*
 - (b) *of order p if P is extra-special of exponent p , or extra-special of exponent p^2 and order at least p^7 , or almost extra-special of order p^6 .*
 - (c) *cyclic of order p^2 if P is almost extra-special of order at least p^8 .*

Proof. We keep Notation 3.16 throughout. We know from Theorem 3.17 that $Cl_1(\mathbb{Z}P) \cong K \times Cl_1(\mathbb{Z}(P/N))$. Moreover $Cl_1(\mathbb{Z}(P/N))$ is elementary abelian of rank $k - 1$, so Assertion 1 follows from Theorem 3.7.

Moreover, the group K is isomorphic to the quotient of Z by the subgroup generated by the elements $u_{H,g,Y}$, where H is a cyclic subgroup of P , and $g \in C_G(H)$. For such a pair (H, g) ,

$$u_{H,g,Y} = \prod_{x \in D} \overline{n_{g,x}}$$

where D is a chosen set of representatives of those double cosets $HxN_P(Y)$ in P for which $H^x \cap N_P(Y) \leq Y$. For each $x \in D$, the element $n_{g,x} \in N_P(Y)$ is chosen such that $gx = h_{g,x}\sigma_g(x)n_{g,x}$, where σ_g is the permutation of D induced by left multiplication by $g \in C_P(H)$, and $h_{g,x} \in H$. The image $\overline{n_{g,x}}$ of $n_{g,x}$ in $N_P(Y)/Y$ is well defined by this equality, thanks to the condition $H^x \cap N_P(Y) \leq Y$.

Suppose that $u_{H,g,Y}$ is non zero. We can apply Lemma 3.19: there is a set D of representatives of those double cosets $HxN_P(Y)$ in P for which $H^x \cap N_P(Y) \leq Y$, and a subgroup X_1 of X_0 of index at most p such that $DX_1 = D$. Then for $x \in D$, we have $gx = h_{g,x}\sigma_g(x)n_{g,x}$, and for $x_1 \in X_1$

$$gxx_1 = h_{g,x}\sigma_g(x)n_{g,x}x_1 = h_{g,x}\sigma_g(x)x_1n_{g,x}[n_{g,x}, x_1],$$

and $n_{g,x}[n_{g,x}, x_1] \in N_P(Y) = ZY$. In other words we have $\sigma_g(xx_1) = \sigma_g(x)x_1$ and we can take $n_{g,xx_1} = n_{g,x}[n_{g,x}, x_1]$. Choosing a set E of representatives of cosets D/X_1 , this gives

$$\begin{aligned} u_{H,g,Y} &= \prod_{\substack{x \in E \\ x_1 \in X_1}} \overline{n_{g,xx_1}} = \prod_{\substack{x \in E \\ x_1 \in X_1}} \overline{n_{g,x}[n_{g,x}, x_1]} \\ &= \prod_{x \in E} \prod_{x_1 \in X_1} \overline{n_{g,x}[n_{g,x}, x_1]} \\ &= \left(\prod_{x \in E} \overline{n_{g,x}}^{|X_1|} \right) \left(\prod_{x \in E} \overline{[n_{g,x}, \prod_{x_1 \in X_1} x_1]} \right). \end{aligned}$$

Now $\prod_{x_1 \in X_1} x_1 = 1$, since X_1 has odd order. Hence

$$(3.21) \quad u_{H,g,Y} = \prod_{x \in E} \overline{n_{g,x}}^{|X_1|}.$$

If $|X_1| \geq |Z|$, since $\overline{n_{g,x}} \in Z$ for any $x \in E$, we then have $u_{H,g,Y} = 0$ in additive notation. This is the case if

- either $|Z| = p$ and $|X_0| \geq p^2$, i.e. if P is extra-special of exponent p and order at least p^5 , or extra-special of exponent p^2 and order at least p^7 ,
- or if $|Z| = p^2$ and $|X_0| \geq p^3$, i.e. if P is almost extra-special of order at least p^8 .

In each of these cases, we have $u_{H,g,Y} = 0$ for any cyclic subgroup H of P and any $g \in C_P(H)$. It follows that $K = Z$ in this case, as was to be shown.

So we are left with the special cases where P is either extra-special of order p^5 and exponent p^2 , or almost extra-special of order p^6 .

Suppose first that P is extra-special of order p^5 and exponent p^2 . Then we have $X = C \times X_0$, where $C \cong C_{p^2}$ and $X_0 \cong C_p$. On the other hand $Y \cong (C_p)^2$ in this case. We take $H = X_0$, and we take for g a generator of C , so indeed $g \in C_P(H)$. Now $H \not\leq ZY$, so $H^x \cap ZY = 1 \leq Y$ for any x in P . Moreover $H \backslash P / ZY = H \backslash XY / ZY \cong H \backslash X / Z \cong C / Z$, so we can take a set D of representatives of these double cosets consisting of a set of representatives of C / Z , e.g. $D = \{1, g, g^2, \dots, g^{p-1}\}$. Now for $x = g^i$ with $0 \leq i \leq p-2$, we have $gx = g^{i+1} \in D$, so $n_{g,x} = 1$. But for $x = g^{p-1}$, we have $gx = g^p = 1 \cdot g^p$, so $n_{g,x} = g^p$ in this case. It follows that $u_{H,g,Y}$ is equal to g^p , which is a generator of Z . Hence K is trivial in this case, as was to be shown. In this case $\text{Def}_{P/N}^P : Cl_1(\mathbb{Z}P) \rightarrow Cl_1(\mathbb{Z}(P/N))$ is an isomorphism.

Suppose now that P is almost extra-special of order p^6 . Then we have $C = Z \cong C_{p^2}$ and $X_0 \cong (C_p)^2$. In this case, Equation 3.21 shows that $u_{H,g,Y}$ is equal to $v_{H,g}^{|X_1|}$ for some $v_{H,g} \in Z$, for any cyclic subgroup H of P and any $g \in C_P(H)$. Moreover X_1 has at least order p , since X_0 has order p^2 . It follows in additive notation that $u_{H,g,Y} \in pZ$.

But on the other hand, write $X_0 = A \times B$, where A and B have order p . If we take $H = B$, and for g a generator of Z , then $g \in C_P(H)$. Moreover $H \not\leq ZY$, so $H^x \cap ZY = 1 \leq Y$ for any x in P . Furthermore $H \backslash P / ZY = X / ZH \cong A$, so A is a set of representatives of the double cosets $H \backslash P / ZY$. But for $a \in A$, we have $ga = ag$, so $n_{g,a} = g \in Z$. It follows that $u_{H,g,Y} = g^{|A|} = g^p$. Hence the subgroup of Z generated by all the elements $u_{H,g,Y}$ is equal to pZ , so $K \cong Z/pZ \cong C_p$ in this case, as was to be shown. \square

References

- [1] R. C. Alperin, R. K. Dennis, R. Oliver, and M. R. Stein. SK_1 of finite abelian groups, II. *Invent. Math.*, 87:253–302, 1987.
- [2] L. Barker. Genotypes of irreducible representations of finite p -groups. *Journal of Algebra*, 306:655–681, 2007.

- [3] D. J. Benson. *Representations and cohomology II*, volume 31 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 1991.
- [4] S. Bouc. K -theory, genotypes, and p -biset functors. In preparation.
- [5] S. Bouc. *Biset functors for finite groups*. Springer, Berlin, 2010.
- [6] S. Bouc. Fast decomposition of p -groups in the Roquette category, for $p > 2$. In *RIMS Kôkyûroku*, volume 1872, pages 113–121, 2014. arXiv:1403.6092.
- [7] S. Bouc and N. Mazza. The Dade group of (almost) extraspecial p -groups. *Journal of Pure and Applied Algebra*, 192:21–51, 2004.
- [8] J. F. Carlson and J. Thévenaz. Torsion endo-trivial modules. *Algebras and Representation Theory*, 3:303–335, 2000.
- [9] K. Doerk and T. Hawkes. *Finite soluble groups*. Walter de Gruyter, Berlin, 1992.
- [10] D. Gorenstein. *Finite groups*. Chelsea Publishing, New York, 1968.
- [11] J. Guaschi, D. Juan-Pineda, and S. Millán López. The lower algebraic K -theory of the braid groups of the sphere. Preprint, arXiv:1209.4791, 2012.
- [12] J.-F. Lafont, B. A. Magurn, and I. J. Ortiz. Lower algebraic K -theory of certain reflection groups. *Proceedings of the Cambridge Philosophical Society*, 148:193–226, 2010.
- [13] R. Oliver. *Whitehead groups of finite groups*. Cambridge University Press, U.K., 1988.
- [14] N. Romero. Computing Whitehead groups using genetic bases. *Journal of algebra*, 450:646–666, 2016.
- [15] P. Roquette. Realisierung von Darstellungen endlicher nilpotenter Gruppen. *Arch. Math.*, 9:224–250, 1958.
- [16] J.-P. Serre. *Linear representations of finite groups*. Springer-Verlag, New York, 1977.
- [17] F. Ushitaki. $SK_1(\mathbb{Z}[G])$ of finite solvable groups which act linearly and freely on spheres. *Osaka Journal of Mathematics*, 28(1):117–127, 1991.
- [18] F. Ushitaki. A generalization of a theorem of Milnor. *Osaka Journal of Mathematics*, 31:430–415, 1994.

- [19] J. H. C. Whitehead. Simple homotopy types. *American Journal of Mathematics*, 72:1–57, 1950.

Serge Bouc, CNRS-LAMFA, 33 rue St Leu, 80039, Amiens, France.
`serge.bouc@u-picardie.fr`

Nadia Romero, DEMAT, UGTO, Jalisco s/n, Mineral de Valenciana, 36240,
Guanajuato, Gto., Mexico.
`nadia.romero@ugto.mx`